Excessive Secrecy Constipates Information Flow

S.R.Brophy
19 April 2007

The problem of overclassification is not new. However, oversight of the implementation of federally mandated information sharing initiatives has refocused concern on a perennial challenge—overclassification and pseudoclassification. As Lee Hamilton said in a 2006 opinion article, "You might say the motto is: when in doubt classify."[1]

Driving Forces

The U.S. National Commission on Terrorist Attacks Upon the United States (the 9-11 Commission) emphasized the importance of information sharing in combating terrorism and ensuring homeland security.[2] The two statutory mandates driving information sharing initiatives, and thus increased focus on classification regimes, are the 2002 Homeland Security Act and the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). Section 892 of the Homeland Security Act requires the President to prescribe and implement procedures under which federal agencies can share homeland security information with other federal agencies, as well as the appropriate state and local personnel.[3] Section 1016 of the IRTPA mandates an even more extensive information sharing regime.[4] It requires the President to facilitate the sharing of terrorism information by establishing an Information Sharing Environment (ISE) that combines policies, procedures, and technologies that link people, systems, and information among all federal, state, local, and tribal entities, and the private sector.

Information sharing enhances the security of the United States because the ability to share terrorism related information unifies the efforts of federal, state, and local government agencies, and the private sector in preventing terrorist attacks. However, the ISE is plagued by overclassification and pseudoclassification, both of which are barriers to information sharing. Homeland Security Chief Intelligence Officer Charles E. Allen recently stated that there is "a continued proclivity towards overclassifying intelligence," and that he and his staff are working hard to institutionalize the Director of National Intelligence's "principle of responsibility to provide."[5] Assistant Commanding Officer of Counterterrorism of the Los Angeles Police Department's Criminal Intelligence Bureau also recently lamented, "More than five years after the tragic events of September 11, local law enforcement involvement [in the fight against international terrorism] has still not been fully embraced because of the impediment of information sharing and the overclassification of intelligence."[6]

[1] Hamilton, Lee H. "When Stamping Secret Goes too Far." *Christian Science Monitor*. February 22, 2006.
[2] U.S. National Commission on Terrorist Attacks Upon the United States. *The 9-11 Commission Report*. Washington: GPO, 2004. p. 416-419.
[3] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.
[4] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638. at http://www.nctc.gov/docs/pl108_458.pdf
[5] Allen, Charles E. Testimony to Congress, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. March 14, 2007. at http://homeland.house.gov/SiteDocuments/20070314172258-47553.pdf
[6] Downing, Michael P. Testimony to Congress, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. March 22, 2007.

The Classification Regime

The purpose of the classification system is to restrict the dissemination of certain information of which the unauthorized disclosure of would result in harm to the United States and its citizens. Classified information falls into two main categories. Information can be classified by the authority of Executive Order 12598, as amended, as Top Secret, Secret, or Confidential.[7] Or, information that does not meet the standards established by the executive order, but that an agency considers sufficiently sensitive to warrant restricted dissemination, is classified as Sensitive but Unclassified (SBU). The problem of overclassification refers to the classification of information that should not have been classified in the first place or that was given a higher than necessary level of classification. The challenge of pseudoclassification refers to the improper or overuse of the SBU designation.

Limiting the quantity of classified information is thought to serve five main purposes.[8] First, it promotes a more informed citizenry. Second, it is a means for effecting accountability for government policies and practices. Third, it is a mechanism for realizing oversight of government operations. Fourth, it is a way to achieve efficiency in government management; and fifth, limiting the amount of security classified information allows the ISE to be effectively realized.

Classification is, according to Director of the Information Security Oversight Office (ISOO) J. William Leonard, "a fundamental tool at the Government's disposal to provide for the 'common defense'." However, Leonard continues, "As with any tool, the classification system is subject to misuse and misapplication."[9] In her March 22, 2007 testimony to the House subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, National Security Archive General Counsel Meredith Fuchs highlighted problems with the SBU designation.[10] A National Archive audit of the policies used by agencies to protect SBU information resulted in the identification of 28 different policies (among the 37 agencies targeted) for protection of SBU information. The 2006 GAO Report *Information Sharing* reported 56 different designations for SBU information among the 26 agencies it surveyed. For example, the Department of Energy (DOE) may mark documents with SBU information as Official Use Only (OUO), or it may choose to use another one of its *sixteen* designations for SBU information. The Department of Defense (DoD) uses the designation For Official Use Only (FOUO), and the Department of Homeland Security uses the designation Protected Critical Infrastructure Information (PCII).

This lack of consistency is troubling. Lack of a government wide comprehensive interoperable SBU designation classification system interferes with information sharing because different agencies will be classifying different information under different labels, or classifying different

[7] Executive Order 12598, as amended by President Bush on March 25, 2003 at http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html

[8] Relyea, Harold C. "Security Classified and Controlled Information: History, Status and Emerging Management Issues." *CRS Report for Congress* RL 33494. Updated March 8, 2007.

[9] Leonard, William J. Testimony to Congress, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. March 22, 2007.

[10] Fuchs, Meredith. Testimony to Congress, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. March 22, 2007.

information under the same labels. Indeed, the 2006 GAO report *Information Sharing* stated that half of the agencies covered reported encountering challenges in sharing SBU info.[11] Government wide policies and procedures that specifically describe the criteria for use of the SBU designation and the uniform use of the same designation would significantly alleviate these challenges.

A lack of internal controls is another problem plaguing the SBU system. This results in an increased risk that a designation will be misapplied, thereby unnecessarily restricting materials that could have been released or inadvertently releasing materials that should be restricted. The GAO reported that most agencies do not have limits on whom and how many employees have authority to make designations.[12] In addition, the report found an absence of training for employees making designation decisions and an absence of periodic reviews to verify proper use of the designation. In her House testimony, Fuchs highlighted the fact that, unlike traditional classified records which are subject to the Freedom of Information Act (FOIA), there is no official oversight of the use or impact of the SBU system. The government wide audit of federal agency FOIA performance *Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information* concluded "The diversity of policies, ambiguous or incomplete guidelines, lack of monitoring, and decentralized administration of information controls on unclassified information is troubling from the perspectives of safety, security, and democracy."[13]

However, certain agencies have implemented their own internal control mechanisms. For example, a Department of Energy employee designating a document is required to place an OUO stamp on the front page of the document.[14] That stamp has a space where the employee must identify which FOIA exemption is believed to apply, as well as a place for the employee's name and organization. This policy encourages accountability and consistency. However, when the GAO recommended the universal application of this policy the DoD rejected the idea that personnel designating a document as FOUO also mark the document with the FOIA exemption used to determine that the information should be restricted. Nevertheless, it is worth noting that the President has mandated the standardization of procedures for designating, marking, and handling SBU information across the Federal Government.[15] Unfortunately, it has not been realized.

The traditional classification system is also not without faults. There is a culture of secrecy within the intelligence community which is widely based on the "need to know" principle. In the 2005 National Intelligence Strategy, John Negroponte acknowledged that while such institutional cultures had developed for good reasons, all cultures either evolve or expire; and "the time has come for U.S. domestic and foreign intelligence cultures to grow stronger by growing

[11] GAO Report: *Information Sharing*. GAO-06-385. March 2006. at http://www.gao.gov/new.items/d06385.pdf

[12] GAO Report: *Information Sharing*. GAO-06-385. March 2006. at http://www.gao.gov/new.items/d06385.pdf

[13] National Security Archive. *Pseudo-Secrets: A Freedom of Information Audit of the U.S. Government's Policies on Sensitive Unclassified Information.* March 14, 2006. at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/SBU%20Report%20final.pdf

[14] GAO Report: Managing Sensitive Information. GAO-06-369. March 2006. at http://www.gao.gov/new.items/d06369.pdf

[15] Bush, President George W. Memorandum for the Heads of Executive Departments and Agencies. December 16, 2005. at http://www.fas.org/sgp/news/2005/12/wh121605-memo.html

together."[16] While few would argue against the idea that certain information needs to be classified, there is broad consensus that far too much information is classified.[17] This prohibits information sharing, which is crucial to enhancing homeland security. In addition, it dilutes the entire classification system whose purpose is to protect truly sensitive national security intelligence.

Another issue looms large in the classification regime. There have long been accusations that certain material is classified not out of concern for national security, but to prevent possible government embarrassment.[18] However, the Executive Order explicitly forbids the classification of material with the intent to, for example, conceal violations of law, inefficiency, administrative errors, or to prevent embarrassment of a person, organization or agency. Strict oversight and periodic reviews help curb such exploitation of the classification regime.

The 2004 IRTPA offered a solid recommendation to help promote the ISE. It recommended that guidelines be implemented to ensure that information is in its most shareable form.[19] Both the President and Negroponte have also called for the establishment of policies that reflect the need-to-share (versus need-to-know) principle. For example, tearlines could be used. Tearlines separate out data from the sources, and the methods by which data are obtained. This protects the source while allowing interagency exploitation of potentially illuminating intelligence. For intelligence agencies to be able to effectively recruit human resources and obtain assistance from foreign intelligence services, sources must be assured total confidentiality. Thus, a tearline system would remove source exposure from the equation (theoretically at least), and allow for increased information sharing. In 2004 then Secretary of State Colin Powell stated, "Intelligence is another name for information, and information isn't useful if it does not get to the right people in a timely fashion."[20]

The goal of reforming information control programs is to establish a responsible classification system and a committed declassification program. Leonard offers certain recommendations which would increase the integrity of the traditional classification regime. Among these are the need for agencies to 1)provide specific clear updated quality classification guidelines that will increase accurate classification decisions, 2) emphasize to all authorized holders of classified information the affirmative responsibility they have under the Executive Order to challenge the classification status of information they believe is improperly classified, 3) appoint impartial officials whose sole responsibility is to seek out inappropriate instances of classification and to encourage others to adhere to their individual responsibility to challenge classification, as appropriate, 4) ensure the routine sampling of recently classified material to determine the

[16] Negroponte, John. "The National Intelligence Strategy of the United States of America: Transformation Through Integration and Innovation." *Office of the Director of National Intelligence*. October 2005. at http://www.intelligence.gov/national_intelligence_strategy.pdf

[17] Armstong, Scott. Testimony to Congress, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. March 22, 2007.

[18] Griswold, Erin. "Secrets Not Worth Keeping." *The Washington Post*. February 15, 1989.

[19] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638. at http://www.nctc.gov/docs/pl108_458.pdf

[20] Powell, Colin. "Intelligence Reform." FDCH Federal Department and Agency Documents-Regulatory Intelligence Data. *U.S. Department of State.* September 13, 2004.

propriety of classification and the application of full and proper markings, and to track trends and make adjustments as necessary, and 5) to ensure that information is declassified as soon as it no longer meets the standards for classification.[21]

The Short of It

Information sharing barriers, such as overclassification and pseudoclassification, can only be overcome through a community wide commitment to the need-to-share principle. Key reforms to achieving this goal include:

1) The need to establish government wide policies and procedures that specifically describe the criteria for the use of the SBU designation, and the uniform use of the same designation throughout government agencies.
2) Internal controls such as increased training and periodic reviews to ensure the integrity of both the traditional and SBU classification systems.
3) Encouraging the need-to-share principle within the intelligence community.
4) Use of tearlines to provide information in its most shareable form.
5) Increased oversight and periodic reviews aimed specifically at preventing or identifying improper instances of classification, especially instances where material has been classified in an attempt to prevent embarrassment of a person or agency.
6) A responsible and efficient declassification program.

While a list of necessary reforms is easy to write, the ability to overcome entrenched tendencies is what will ultimately dictate the degree of success the intelligence community achieves in regards to establishing a truly interoperable ISE. The key is to find an appropriate balance between secrecy and sharing, which can only be realized through effective leadership and clear guidelines.

[21] See March 22, 2007 testimony as noted above.